IN THE CLAIMS

1. (currently amended) An information processing system for distributing encrypted message data ~~capable of being used only in not less than one device selected~~, said ~~individual device~~ system comprising:

a receiving device, including:

encryption processing means for holding a ~~different~~ key set specific to said receiving device and that includes ~~of a~~ node keys ~~peculiar to~~ associated with each node in a path from a top key of a hierarchical tree structure to a leaf node associated with said receiving device, ~~with~~ the hierarchical tree structure having a plurality of different devices as its leaves and having an associated leaf key ~~peculiar to~~ for each device, and ~~executing~~ for decrypting ~~process on said~~ encrypted message data distributed to ~~a~~ said receiving device by using said key set; and

a distributing device, including:

~~wherein a~~ message data ~~distributing~~ generating means for generating~~es~~ a renewal node key ~~into~~ by which at least one of ~~the~~ a plurality of node keys is renewed by said receiving device, the plurality of node keys and a plurality of leaf keys being respectively associated with ~~in~~ a group constituted ~~by~~ of nodes and leaves ~~connected at subordinate of a top node which is one node~~ of the hierarchical tree structure, ~~is renewed~~ and for generating an enabling key block (EKB) within ~~into~~ which said renewal node key is encrypted ~~with a~~ using one of the plurality of node keys or ~~a~~ one of the plurality of leaf keys ~~in said group~~, and

message data distributing means for ~~generating and~~ distributing ~~a~~ message data that includes data in which content is encrypted with a content key, data in which the content key is encrypted by a content encryption key, and a link to data in which the content encryption key is encrypted by the enabling key block (EKB) and to which other message data is linked, the content encryption key being said renewal node key.

2. (currently amended) The information processing system according to claim 1 wherein said encryption processing means in said receiving device obtains said renewal node key by the processing of said enabling key block (EKB) and executing decrypting of said encrypted message data by the renewal node key obtained.

3. (cancelled)

4. (currently amended) The information processing system according to claim 1 wherein said message data ~~is~~ includes an authentication key used in the authentication processing.

5. (currently amended) The information processing system according to claim 1 wherein said message data ~~is~~ includes a key for ~~generateing~~ generating an integrity check value (ICV) of the content.

6. (currently amended) The information processing system according to claim 1 wherein said message data ~~is~~ includes a program code.

7. (currently amended) The information processing system according to claim 1 wherein said message data distributing means distributes said enabling key block (EKB) in place of the link~~and an encrypted data comprising a content key usable as a decryption key for decrypting content data as said message data and an encrypted content encrypted by said content key~~.

8. (currently amended) The information processing system according to claim 1 wherein said message data distributing means and said receiving device respectively have an authentication processing means for executing authentication processing, and ~~wherein~~ a distribution of said message data is performed on the condition that authentication processing

between said message data distributing means and said receiving device has been completed.

9. (currently amended) The information processing system according to claim 1 wherein there exists a different intermediate device between said message data distributing means and said receiving device, and ~~wherein~~ said message data distributing means generates and distribut~~ing~~es an enabling key block (EKB) and ~~an~~ encrypted message data that can be decrypted only in target devices targeted for distributing said message data.

10. (original) The information processing system according to claim 1 wherein said hierarchy tree structure includes a category group constituted as a group, with one node as a top node, containing nodes and leaves connected at subordinate of said top node;

wherein said category group is constructed as a set of devices that belong to a category defined solely by a kind of a device, a kind of a service or a kind of a managing means.

11. (original) The information processing system according to claim 10 wherein said category group further includes one or more sub-category groups in the lower stage of said hierarchy tree structure;

wherein said sub-category group is constructed as a set of groups that belong to a category defined solely by a kind of a device, a kind of a service, a kind of a managing means.

12. (currently amended) An information processing method for distributing ~~from a message data distributing means~~ encrypted message data ~~capable of being used only in not less than one device selected~~, said method comprising:

a message data generating ~~distributing~~ step of generating a renewal node key ~~into~~ by which at least one of a plurality of node keys is renewed, the plurality of node keys and a plurality of leaf keys being respectively associated with ~~in~~ a group constituted ~~by~~ of nodes and leaves connected at positions subordinate to ~~of~~ a top node ~~which is one node~~ of a ~~the~~ hierarchical tree structure having a plurality of different devices as its leaves ~~is renewed~~, and generating an enabling key block (EKB) ~~into~~ within which said renewal node key is encrypted ~~with a~~ using one of the plurality of node keys or ~~a~~ one of the plurality of leaf keys; ~~in said group, and generating and~~

a message data distributing step of distributing ~~a~~ message data that includes data in which content is encrypted by a content key, data in which the content key is encrypted by a content encryption key, and a link to data in which the content encryption key is encrypted by the enabling key block (EKB) and to which other message data is linked, the content encryption key being said renewal node key; and

a decrypting ~~processing~~ step of ~~executing~~ decrypting, at a given one of the plurality of different devices, ~~processing on~~ said encrypted message data ~~by~~ using an associated key set ~~in each~~ stored in that device and data in which the content encryption key is encrypted by the enabling key block (EKB), each one of the plurality of different devices holding ~~said~~ a different associated key set formed of ~~a~~ the node keys ~~peculiar~~ specific to each node in a path from the top key of said hierarchical tree structure to the leaf node specific to that device and a holding leaf key ~~peculiar~~ specific to ~~each~~ that device.

13. (original) The information processing method according to claim 12 wherein said decrypting processing step includes a renewal node key obtaining step of obtaining said renewal node key by processing of the enabling key block (EKB); and

a message data decrypting step for executing decryption of the encrypted message data by said renewal node key.

14. (cancelled)

15. (currently amended) The information processing method according to claim 12 wherein said message data ~~is~~ includes an authentication key used in the authentication processing.

16. (currently amended) The information processing method according to claim 12 wherein said message data ~~is~~ includes a key of generating an integrity check value (ICV) of contents.

17. (currently amended) The information processing method according to claim 12 wherein said message data ~~is~~ includes a program code.

18. (cancelled)

19. (currently amended) The information processing method according to claim 12 further comprising ~~wherein said message data distributing means and said device respectively have~~ an authentication processing ~~means~~ step for executing authentication processing, and

wherein ~~a~~ said distribution of said message data is performed on the condition that said authentication processing step ~~between said message data distributing means and said device~~ has been completed.

20. (currently amended) The information processing method according to claim 12, ~~wherein there exists a different intermediate device between said message data distributing means and said device, and~~ wherein said message data distributing ~~means~~ step generates and distributes an enabling key block (EKB) and an encrypted message data that can be decrypted only in a target device targeted for ~~distributing~~ receiving said message data.

21. (currently amended) An information recording medium having stored therein data, ~~storing~~ comprising:

a renewal node key ~~into~~ by which at least one of a plurality of node keys is renewed, the plurality of node keys and a plurality of leaf keys being respectively associated with

~~in~~ a group constituted ~~by~~ of nodes and leaves connected at positions subordinate ~~of~~ to the top node ~~which is one node~~ of ~~the~~ a hierarchical tree structure having a plurality of different devices as its leaves; ~~is renewed and~~

an enabling key block (EKB) ~~into~~ within which said renewal node key is encrypted ~~by a~~ using one of the plurality of node keys or ~~a~~ using one of the plurality of leaf keys ~~in said group~~; and

a message data that includes data in which content is encrypted by a content key, data in which the content key is encrypted by a content encryption key, and a link to data in which the content encryption key is encrypted by the enabling key block (EKB) and to which other message data is linked, the content encryption key being said renewal node key.

22. (currently amended) The information recording medium according to claim 21, ~~wherein said message data is a content key used for decrypting contents, and~~wherein said information recording medium stores an encrypted content encrypted by said renewal node key.

23. (original) The information recording medium according to claim 22 wherein said information recording medium stores correspondence data for relating a content with an enabling key block (EKB) used for obtaining a content key corresponding to said content.

24. (original) The information recording medium according to claim 21 wherein said information recording medium stores an integrity check value (ICV) of contents.

25. (currently amended) A program providing medium for providing a computer program for carrying out a method of ~~executing~~ decrypting ~~process of~~ encrypted content ~~data on a computer system~~, said ~~computer program~~ method comprising:

a renewal node key obtaining step of obtaining a renewal node key by linking to enabling key block (EKB) data within which the renewal node key is encrypted and to which other content is linked, decrypting ~~process of an~~ the enabling key block (EKB) ~~into which said renewal node key~~ using ~~into which~~ at least one of ~~the~~ a plurality of node keys or one of a plurality of leaf keys, ~~in~~ the plurality of node keys and the plurality of leaf keys being respectively associated with a group constituted ~~by~~ of nodes and ~~a leaf~~ leaves connected at positions subordinate ~~of~~ to ~~the~~ a top node ~~which is one node~~ of ~~the~~ a hierarchical tree structure having a plurality of different devices as its leaves, ~~is~~ at least one of the plurality of node keys being renewable~~ed~~ ~~is encrypted with a node key or a leaf key in a group on a~~ by the renewal node key;

a step of ~~executing~~ decrypting, ~~process by~~ using said renewal node key, to obtain a content key ~~used as a decryption key for said encrypted content~~; and

a step of ~~executing~~ decrypting~~on~~ ~~of~~ said encrypted content ~~by~~ using said content key.

26. (currently amended) An information processing method for distributing encrypted message data ~~capable of being used only in not less than one device selected~~, said method comprising ~~the steps of~~:

generating a renewal node key ~~into~~ by which at least one of a plurality of node keys is renewed, the plurality of node keys and a plurality of leaf keys being respectively associated with ~~in~~ a group constituted ~~by~~ of nodes and leaves connected at positions subordinate to ~~of~~ a top node ~~which is one node~~ of a ~~the~~ hierarchical tree structure having a plurality of different devices as its leaves; ~~is renewed, and~~

generating an enabling key block (EKB) ~~into~~ within which said renewal node key is encrypted ~~by a~~ using one of the plurality of node keys or ~~a~~ one of the plurality of leaf keys~~ in said group~~; and

generating a message data that includes data in which content is encrypted with a content key, data in which the content key is encrypted by a content encryption key, and a link to data in which the content encryption key is encrypted by the enabling key block (EKB) and to which other message data is linked, the content encryption key being said renewal node key, to distribute ~~it~~ the message data to devices.

27. (cancelled)

28. (currently amended) The information processing method according to claim 26 wherein said message data ~~is~~ includes an authentication key used in the authentication processing.

29. (currently amended) The information processing method according to claim 26 wherein said message data ~~is~~ includes a key of generating an integrity check value (ICV) of contents.

30. (original) The information processing method according to claim 26 wherein said enabling key block (EKB) and an encrypted data is distributed, said encrypted data comprising a content key usable as a decryption key for decrypting content data as said message data and an encrypted content encrypted with said content key.

31. (currently amended) An information processing method, comprising:

a renewal node key obtaining step of obtaining a renewal node key by linking to enabling key block (EKB) data within which the renewal node key is encrypted and to which various contents are linked, decrypting ~~processing of an~~ the enabling key block (EKB) ~~into which said renewal node key into which~~ using at least one of ~~the~~ a plurality of node keys or one of a plurality of leaf keys, the plurality of node keys and the plurality of leaf keys being respectively associated with ~~in~~ a group constituted ~~by~~ of nodes and ~~a leaf~~ leaves connected ~~to a~~ at positions subordinate ~~of~~ to a top node ~~which is one node~~ of a hierarchical tree structure having a plurality of different devices as leaves, ~~is~~ at least one of the plurality of node keys being renewed by the renewal node key~~is encrypted with a node key or a leaf key in said group~~;

a content key obtaining step of ~~executing~~ decrypting~~on~~, ~~process with~~ using said renewal node key, to obtain a content key~~ used as a decryption key for said encrypted content~~; and

an executing step of ~~executing~~ decrypting ~~of~~ said encrypted content ~~by~~ using said content key.

32. (cancelled)

33. (cancelled)